REMARKS

The Examiner has rejected Claim 9 under 35 U.S.C. 101 as being directed to non-statutory subject matter. Applicant notes that such rejection is overcome in view of the clarification made to such claim.

The Examiner has rejected Claim 8 under 35 U.S.C. 112, second paragraph, as being indefinite. Such rejection is deemed avoided by virtue of the clarifications to such claim made hereinabove.

The Examiner has rejected Claims 1-23 under 35 U.S.C. 102(b) as being anticipated by Arnold et al. (U.S. Patent No. 5,440,723). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to independent Claims 1, 9-11, and 17.

With respect to independent Claims 1, 9 -10 and 23, the Examiner has relied on the following excerpt from Arnold to make a prior art showing of applicant's claimed "quarantining the potentially malicious content of the network communications" (see this or similar, but not identical claim language in each of the foregoing claims).

> "At this point, there are one or more sections of a virus program (or a set of different viruses) that are marked as being substantially "invariant". However, even if a given section of the virus program is common to all copies which have been obtained in Step C, this does not guarantee that the section will appear in its entirely in every instance of the virus. The purpose of Block B is to filter out portions of the "invariant" sections which by their nature are more likely to be variable. As a general rule, non-executable "data" portions of programs, which can include representations of numerical constants, character strings, screen images, work areas for computations, addresses, etc., tend to be more likely to vary from one instance of the program to another than "code" portions, which represent machine instructions." (Col. 7, line 59-Col. 8, line 6)

Applicant respectfully asserts that the above excerpt from Arnold merely discloses marking sections of a virus program as being substantially invariant. Clearly,

simply marking sections of a virus program does not meet "quarantining" in the context claimed by applicant. In addition, once such sections are marked, only those portions are filtered out of the program (see item B of Figure 4 and Col. 7, lines 25-27). Thus, Arnold merely suggests marking and filtering, but not any sort of quarantining.

Nevertheless, despite such deficiencies in the prior art and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of dependent Claim 7 into independent Claims 1, 9 and 10. Such subject matter is also included in independent Claim 23, as originally filed.

With respect to Claim 7, now incorporated into each of the foregoing claims, the Examiner has relied on item E of Figure 2 and Col. 4, lines 35-52 in Arnold to meet applicant's claimed technique "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content." However, applicant notes that item E of Figure 2 and the above excerpt relied on by the Examiner merely teach extracting a viral signature from code and adding it to a scanner's database. Simply extracting a viral signature from code and adding it to a database, as disclosed in Arnold, does not even suggest quarantining, in the context claimed by applicant. Furthermore, applicant notes that Arnold also fails to teach any sort of quarantining "until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content," as claimed by applicant.

With respect to independent Claim 11, applicant respectfully asserts that "quarantining the potentially malicious content of the network communications," as claimed by applicant, is not met by the Arnold references for the reasons noted with respect to independent Claims 1, 9-10 and 23 above. In addition, the Examiner has relied on the following excerpt from Arnold to make a prior art showing of applicant's claimed "delivering the network communications over the network after a predetermined delay" (see Claim 11).

> "If a predetermined amount of time has elapsed and no virus samples have been captured by decoy programs, the user can receive a message (Block E) to the effect that an executable was modified, but that no further evidence of a virus was discovered. If no virus samples have been captured, but other executables were modified during the course of executing Block J, the user receives a message indicating that there is strong evidence of a virus, but that the immune system has as yet been unable to capture a sample." (Col. 25, lines 32-40)

Applicant respectfully asserts that the above excerpt from Arnold only teaches transmitting a message to a user after a predetermined amount of time elapses which states that an executable was modified or that there is strong evidence of a virus. Clearly, transmitting such a message in no way even suggests delivering the network communications over the network where the network communications contain potentially malicious content (see the entire context of Claim 11).

Nevertheless, despite such deficiencies in the prior art and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of dependent Claim 16 into independent Claim 11. With respect to Claim 16, the Examiner has relied on item B of Figure 2 and Col. 1, line 45-63 and Col. 25, lines 31-40 to make a prior art showing of applicant's claimed technique "wherein the delay is for allowing quarantining of the potentially malicious content until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content." Applicant respectfully disagrees with such assertion.

Specifically, applicant respectfully asserts that item B of Figure 2 merely depicts scanning for known viruses and that such excerpts relied on by the Examiner simply disclose sending a message to a user after a predetermined amount of time (see Col. 25, lines 31-40) and virus scanning (Col.1, lines 45-63). Clearly there is simply no disclosure of a delay that allows for "quarantining of the potentially malicious content until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content."

With respect to independent Claim 17, applicant has incorporated the following claim language into such claim:

> "delivering the network communications from the quarantine over the network in response to a request from a user;
>
> wherein it is determined whether the user is authorized, and the network communications are delivered only if the user is determined to be authorized."

Again, applicant respectfully asserts that nowhere in the entire Arnold reference is there any disclosure, or even suggestion of quarantining as noted above with respect to the other independent claims. Furthermore, applicant also respectfully asserts that Arnold also fails to teach determining whether a user is authorized and only delivering network communications if the user is authorized, in the manner currently claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Arnold reference, especially in view of the amendments made hereinabove. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 6 et al., the Examiner has relied on Col. 7, line 22-33 and Col. 7, line 59-Col. 8, line 6 to meet applicant's claimed technique

"wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value." However, applicant asserts that such excerpts only teach comparing virus programs with one another to determine and mark them if they are invariant (i.e. the same), or if they are different with substantial areas in common, sending them for further processing. Clearly, such excerpts completely fail to even mention "electronic mail," let alone identifying electronic mail "as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value," as claimed by applicant (emphasis added).

Again, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested. Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 24-28 below, which are added for full consideration:

"wherein the potentially malicious content is identified utilizing heuristics" (see Claim 24);

"wherein the heuristics include generating a histogram of content that has been sent over the network during a period of time and analyzing the histogram to determine if multiple copies of the potentially malicious content have been sent over the network during the period of time such that the number of copies exceed a predetermined value" (see Claim 25);

"wherein the quarantining includes containing the potentially malicious content and preventing the potentially malicious content from creating damage" (see Claim 26);

"wherein when multiple recipients are to receive a copy of the potentially malicious content, a single copy of the potentially malicious content is quarantined and each of the recipients is placed in a list such that after the content

is determined to be clean based on the testing, the single copy is forwarded to each of the recipients" (see Claim 27); and

"wherein an intended recipient of the network communications is notified that the potentially malicious content is quarantined" (see Claim 28).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P040/01.254.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100